Research Paper | Computer Science | E-ISSN No : 2454-9916 | Volume : 3 | Issue : 2 | Feb 2017

RECTIFICATION OF INFORMATION AND DYNAMIC REALLOCATION OF BLOCKS IN CLOUD

Rahul Pradev.R [1] | Hari. S [1] | Dr. Balakumar. P [2] | Kapila Vani. R. K [3]

[1] Department of Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India.

[2] Professor, Department of Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India.

[3] Assistant Professor, Department of Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India.

ABSTRACT

Cloud computing induced tremendous number of stakeholders who can outsource the resources at various levels. The security implementations towards for the user's satisfaction has been a major challenge for all the cloud service providers. Even though various security methodologies are adopted, there may rise some breaches or lack of concentration or carelessness by the stakeholders, using which the intruders can penetrate and act upon the information over the cloud. To avoid those categories of disasters and to serve the customers back with their initial atomic information, the cloud service is coupled with a third-party verifier. We propose a verifier who monitors the transitions and actions over the cloud in random selections, and performs recovery, if the information has been affected. The intruder's most liked information, over which the corruption occurs, is dynamically reallocated after it is rectified to its initial state by the verifier. Hence, we implement a new architecture, where the verifier is established as an intermediate between the users and the service providers. To enhance security the information is split into blocks and stored in multi-cloud environment, so exact retrieval of the entire information by hackers becomes tedious and impossible.

KEY WORDS: Blocks spilt, dynamic reallocation, multi-cloud, recovery, verifier.

I. INTRODUCTION

The current trend has established a massive hike towards cloud computing. They come up with economic benefits and transparency that suits many of the business organizations as well as users of interest. Business organizations are deeply concerned with reliability of information. Several security policies are established to avoid the breach over the cloud environment. But there are several other issues that is related towards the users end or in-between the communication channels or even the internal threats. Authorization of exact users may become fault when some login or privacy credentials are exposed to the outside world. These simple security threats may not be shown as highly vulnerable, but later they turn into a mound. Cloud organizations are confined towards various laws and legislations to support integrity of information, framed legally to recommend the customers for the utilization of resources. Researches are focused on various hacking techniques over various applications. There are many tools used by the hackers probably invented in some countries. They are defined to penetrate applications and steal data. The main aim of anonymous users is to steal information, when failed, they try with the Distributed Denial of Service attacks.

Imperva Hacker Intelligence initiative report, a well-known cyber security company has exposed some of the breach holes in various popular cloud service providers. They exposed that if a hacker get into client's computer where the services are installed, then they don't require any user login credentials for identity, to access the data. The experts found that, whenever services provide constant access towards the user, they share a security token that is stored over the Windows registry of the client's workstation. A switcher is shared by the hacker through any mode of communication like e-mail or by cookies, which is automatically executed. This switcher replaces the original token with the hacker's token on the client's machine. Now the hacker is granted with access to the cloud account of the victim client. Hence some mechanisms are implemented in this study to avoid the disaster by denial of service attack and recovery from such disasters.

II. RELATED STUDY

There have been research and implementations which involved the monitoring of activities in the cloud environment. This is helpful in creating certificates, which provides a proof for the society on the cloud. And the security is focused by different experts at different levels (based on architecture, entities etc.). Agents are involved to monitor malicious activity that holds the logs of the action, place, time and by whom. Audit trails can take preventive maintenance but the issue lies with the corrective maintenance. Since virtual machines are created, the concern of isolation of the resources towards the users is difficult. Researchers say that even the top-class security lacks are prone to some threats. Monitoring the transfer are carried out by the cloud service provider, but the consideration of actions on the cloud and the attack over the communication cannot be traced by cloud service provider. An independent source should handle these tasks to be transparent to the customers.

III. SECURITY THREATS

Some the security threats that could be identified over the cloud environment are provided below,

1. **Insiders attack:** In this type, the attacker may be involved in the organization and he will have granted with access towards the login credentials of the internal users. This information may be utilized by himself or even be shared to others. Hence the certificate is more helpful to raise the standards of the cloud and to overcome these types of threats.

2. **Link Share:** There are some situations in some of the cloud, where the storage information access could be granted via an URL link. But if the information is sensitive, then the attack over the communication could easily provide the link, that could be accessed by any without any user credentials. This happened in real world, where some drives are used to share links for access by private customers, where there had been some breaches getting the URL, so they could steal the information or inject virus to corrupt the data.

3. **Exposed passwords:** There are many threats that the users may not feel much vulnerable, but they do in some instance. Many attacks like shoulder behind attack or spoofing the communication without the use of keys to be shared, the hackers can easily trace out the passwords and access the cloud. Monitoring the passwords by screen capturing in hand held devices makes the hackers to easily trace the passwords and other credentials. Installation of some applications could disagree with the security and compliance and grants some of the access over the machines to the hackers.

4. **Personal System:** There are many threats when any intruders get into the system of a client. Because tokens of various accounts could be replaced easily by the hacker's tokens. The hackers can access accounts without the user login credentials and this is called “Man-in the cloud”. The intruder can install tools that could do malicious activities like changing the SQL etc. Logging to the system of the client can let many paths to the hackers in accessing various accounts of the user.

5. **Phishing:** This type of attack is carried out by spam or malware, where the exact site of the cloud may be represented to the user. But, in real, there will be slight change in the URL or any content that the user may find difficult to trace it out. Hence if the user logs into it by his original login credentials then the attackers could easily trace the information and could attack over the cloud environment of user. This phishing may also be progressed by sending mails with some URL which may lead to malicious environment. The policies and terms are must to be read carefully to know the service provided by them.

IV. EXISTING METHODOLOGIES

In this section, we discuss about some of the existing mechanisms that are used as proactive maintenance to avoid threats over the cloud.

A. Audit trials: Audit trials are executed to monitor the events that come from different sources. They hold information related to the questions who, where, when and the operation. These are compared to the normal behaviour and if it seems to move in different path, then the action could be blocked or some alternate measures could be implemented.

B. Data Transfer Monitors: DTM are used to monitors API level communication that normally occurs between the cloud services. Some of the information may be private and they are not supposed to be share among the third-parties. Id of the tenants would be passed to the data controller so that they could take necessary actions upon the calls.

C. Agents: Agents are autonomous entities in a particular environment, monitoring the actions and responses to the dynamic changes in the environment. Agents can communicate and can even form groups in order to solve complex issues. Agents must react instantaneously towards the change in infrastructure to detect the attacks or intrusion. Implementing such architecture is possible through connected sensors confined to certain action over the process or events. The detection by one agent may share related information to other agents so the task of repetition is reduced.

V. PROPOSED METHODOLOGIES

In this section, methodologies are discussed in implementing the proposed system. They are,

A. Geographic location: The information stored over the cloud are located irrespective of the location of the servers. The users are not exposed the exact location of the location to avoid the disasters towards the servers. Some cloud service providers maintain additional backup that serves in emergency situations. The information of the users is traversed to different locations based on the availability, type or the package for the user. Even though the information in encrypted before placing over the cloud, the attackers could try all the possible brute force attacks to find the exact cryptographic algorithm and may cease the entire information, if stored in a single location. We proposed the system of storing the information in multi cloud, where the information is divided based on the number of the cloud environment and stored on to it. Hence the act of trying different cryptographic reverse process may not yield the exact full information as they are split into different cloud storage. To enhance even more fine refinement towards the attack of large data over a particular cloud, the data could be divided into small chunks and stored in blocks of fixed size.

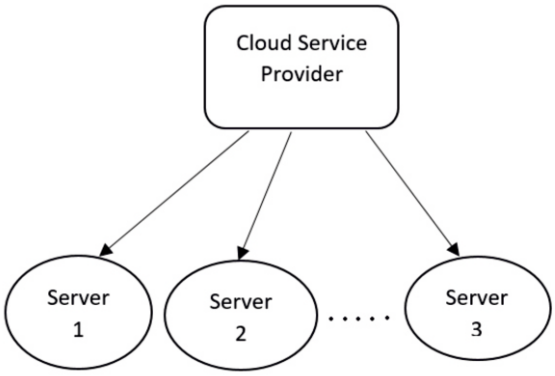


Fig 1. Setting up the required cloud servers

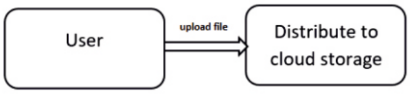
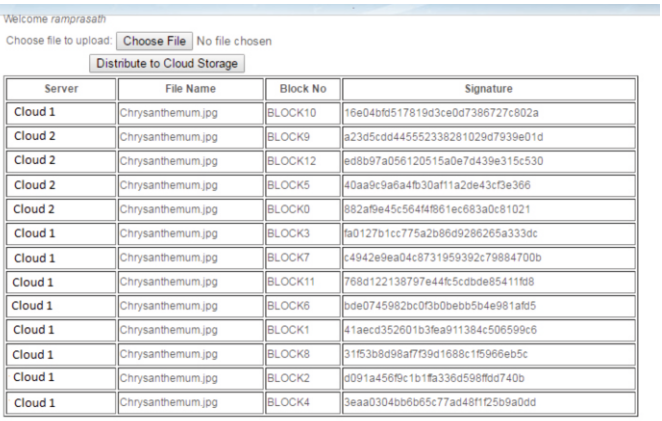


Fig 2. Uploading the file to be split

B. Signature Application and FAT: The blocks are viable to be attacked by hackers, and to find the mark of attack, we include the mechanism of signature for the blocks of information. Signatures are generated for every block of data and are stored in a File Allocation Table(FAT) File system. This FATFS holds the details of the activity that takes place over the cloud. The signature can be generated using any of the cryptographic algorithms. The signatures are even appended to the block of data succeeding a special character. Then they are encrypted and stored on to the blocks. The FAT maintenance is cloud dependent to have a note of the activities over the cloud of various users. The signatures are utilized by the verifier to check the integrity of the data in the blocks.


Welcome *ramprasath*

Choose file to upload: Choose File No file chosen

Distribute to Cloud Storage

Server	File Name	Block No	Signature
Cloud 1	Chrysanthemum.jpg	BLOCK10	16e04bfd517819d3ce0d7386727c802a
Cloud 2	Chrysanthemum.jpg	BLOCK9	a23d5cdd445552338281029d7939e01d
Cloud 2	Chrysanthemum.jpg	BLOCK12	ed8b97a056120515a0e7d439e315c530
Cloud 2	Chrysanthemum.jpg	BLOCK5	40aa9c9a6a4fb30af11a2de43cf3e366
Cloud 2	Chrysanthemum.jpg	BLOCK0	882af9e45c564f4f861ec683a0c81021
Cloud 1	Chrysanthemum.jpg	BLOCK3	fa0127b1cc775a2b86d9286265a333dc
Cloud 1	Chrysanthemum.jpg	BLOCK7	c4942e9ea04c8731959392c79884700b
Cloud 1	Chrysanthemum.jpg	BLOCK11	768d122138797e44fc5cdbde85411fd8
Cloud 1	Chrysanthemum.jpg	BLOCK6	bde0745982bc0f3b0bebb5b4e981afd5
Cloud 1	Chrysanthemum.jpg	BLOCK1	41aecd352601b3fea911384c506599c6
Cloud 1	Chrysanthemum.jpg	BLOCK8	31f53b8d98af7f39d1688c1f5966eb5c
Cloud 1	Chrysanthemum.jpg	BLOCK2	d091a456f9c1b1ffa336d598ffdd740b
Cloud 1	Chrysanthemum.jpg	BLOCK4	3eaa0304bb6b65c77ad48f1f25b9a0dd

Fig 3. Signature generation and block split

Based on the necessity of the cloud infrastructure different kinds algorithms could be implemented towards the encryption and for signatures or identity towards data integrity.

1) SHA-1: SHA-1(Secure Hash Algorithm1) is cryptographic hash function, that produces a 160-bit hash value called message digest. Cryptanalysts suggest that they are prone to vulnerabilities and can be easily detected through brute force attacks.

2) MD-5: MD5 is widely used hash function that is also used to check the data integrity and checksum. They produce 128-bit hash value. They suffer from high vulnerabilities and the checksum can be used to verify for data matching.

3) HMAC: HMAC (Keyed- Hash Message Authentication Code) is a message Authentication code used for data integrity. This algorithm is combined with MD5 or SHA-1 to raise the security and reduce the vulnerabilities.

C. Monitoring and integrity check: The verifier is a third-party agent for assurance of information, is established to monitor the cloud information. The attackers try penetrating and attempting the denial of service attacks that could cause loss or abuse of information. The signatures act as key in determining whether the information in intact. The Cloud service providers provide random blocks of information of different users to the verifier to check the integrity status. Random information is provided in order to avoid the verifier being exposed of the contents of the information of various users, so he might turn to attack the data. The cloud service provider sends the block and its information in the FATFS to the verifier. The role of verifier is to split the signature from the appended block and to generate a signature using same mechanism for the block without signature. Now he verifies the three signatures generated by him, signature from the block and signature from the FATFS. If all the three signatures are same, then the verifier assures that they are complying to the user's original information. If any one of the signatures are mismatched, then the verifier considers as an infected block and implements recovery process.

Alternate approach: As the cloud providers send random blocks of random users, then the probability of the occurrence of the infected blocks are high that are not been identified. Hence the monitoring is conducted as audits for a prefixed time. If any user tries retrieving the information before his chance of data being checked arrives and if his information is corrupted, then he can complaint the cloud admin on retrieval. In such case, the cloud would gain high probability of serving the infected information request since among the large number of users, the complaint has made the cloud to detect the infected data easily. The details regarding to that particular block (block, signature from FATFS) is passed to the verifier. The verifier performs the recovery mechanism and retrieves the exact information.

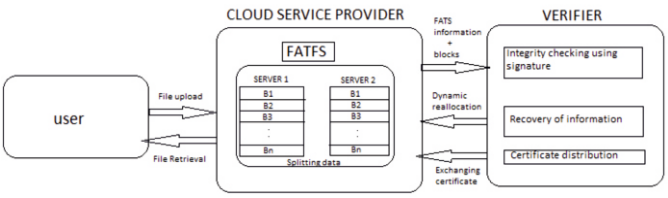


Fig 4. Conceptual architecture

D. Recovery: The recovery mechanism gets back to the initial state of the content that has been uploaded over the cloud. Several recovery mechanisms could be implemented internally by an organization or by an external body. External bodies involve some third-party software applications but there rise even more security related issues while installing the applications.

Hence the same organization could deal with the recovery implementations. The logs are maintained in the FATFS and these logs are used to reverse the process to get back to its initial state. This is termed as "rollback" where the infected information is propagated in the reverse direction to its initial atomic state. Now the user is provided back with the exact information that he stored over the cloud. The verifier instantiates the recovery process by intimating it to the cloud admin. Once the information is rolled back then the FATFS table is reassigned with the new information and signatures.

E. Reallocation: The aim of attacker to attack the information are classified into two types- (i) general interest (ii)Targeting particular individual. If the hacker does abuse of information because of general interest, then he tries attacking random user's information that have the breaches to easily loop into it. Hence the location of that user may not be tracked frequently. But in cases where the attacker tries to steal information or attacks of any specified user, then the probability of trying the same mechanism over the same user is high. This may be related to any business or finance information. Hence the location of the blocks over a single cloud also plays a major role towards security. If the blocks are statically allocated, then the mentioned threat could be easily implemented. We propose dynamic reallocation of the blocks either within the same or different cloud environment. This could avoid tracking the location or overcome the breaches. The block location checking algorithms can be simple by having a status that would trace the located blocks and the cloud. It should be written such that the status should-n't be repeated with same values until all other attempts are tried to return to same status value. Dynamic reallocation appropriately reduces a vast percentage of same information being attacked.

Algorithm 1

Input: Blocks Bi, i<n, where n is the total number of blocks.

Output: Reallocated blocks Bi, i<n, where n is the total number of blocks.

Step 1: Blocks are stored in array like B[0], B[1],….,B[n]

Step 2: Choose any blocks in random manner where all blocks have status="no"

Step 3: Set the status value to "yes" if it is allocated for the block for first time.

```
for(i=0;i<n;i++)
    {
status=" yes";
    }
```

Step 4: Iterate all the blocks checking the status for "no" and assign the reallocated data to those blocks.

Step 5: After all the block's register values are "yes", then the blocks can be reallocated in any random manner but not repeating the same blocks in consecutive allocation.

F. Certification: Providing certificates to the cloud environment by continuous monitoring remains static and doesn't provide any remedial method to the security. The rectification of the infected blocks and the dynamic reallocation of the rectified blocks raises the level of security and acts as a corrective maintenance as well as preventive maintenance. Hence the standard of the certificate stays high compared to the regular auditing certificates that expose security based on activities over the cloud society. This certification is dynamic based on the attacks and recovery from it.

VI. CONCLUSION

The advantages are worth more than general awareness structure by certificates based on the logs or evidences. The trustworthiness of the cloud increases where reliability and integrity is highly achieved. The architecture of the cloud service environment has to be modified by implementing a verifier in-between the communication, at the tier same as the cloud admin. The communication is bonded only with the admin and the verifier. Thus, our system provides remedy to reach the initial information even after attack and avoiding further more attack over the same information.

VII. FUTURE RESEARCH

As the discussion reveals the use of verifier in rectifying the information along with the serving the users, further research must focus on the standard of the verifier. Many new organizations may start establishing verifiers for different cloud computing providers. Hence a common standard has to established by NIST (National Institute of Standards and Technology) or ISO (International organization for Standardization), that could be assurance to all the stakeholders of the cloud. Another enhancement is focused on the separation of the users based on anomaly based detection to ease monitoring and to avoid the threats earlier.

REFERENCES

[1] Sebasitin Lins, Stephan Schneider and Ali sunyaev, "Trust is good,control is better: creating secure clouds by continuous auting, IEEE trans. in cloud computing,2015.

[2] K. M. Khan and Q. Malluhi, "Trust in Cloud Services: Providing More Controls to Clients", Computer, vol. 46, no. 7, pp. 94– 96, 2013.H.

[3] I. Windhorst and A. Sunyaev, "Dynamic certification of cloud services", in Proc. ARES, Regensburg, Germany, 2013.

[4] M. A. Vasarhelyi and F. B. Halper, "The continuous audit of online systems", Auditing, vol. 10, no. 1, pp. 110–125, 1991.

[5] S. Schneider, J. Lansing, F. Gao, and A. Sunyaev, "A taxonomic perspective on certification schemes", in Proc. HICSS, Big Island, Hawaii, USA, 2014, pp. 1–10.

[6] K. Singh, P. J. Best, M. Bojilov, and C. Blunt, "Continuous auditing and continuous monitoring in ERP environments", Inf.

[7] P. Stephanow, C. Banse, and J. Schütte, "Generating Threat

Profiles for Cloud Service Certification Systems", in 17th IEEE High Assurance Systems Engineering Symposium (HASE), 2016.

[8] Q. Fu, J.-G. Lou, Y. Wang, and J. Li, "Execution anomaly detection in distributed systems through unstructured log analysis", in Proc. ICDM, Miami, Florida, USA, 2009, pp. 149–158.

[9] T. C. Du, E. Y. Li, and E. Wei, "Mobile agents for a brokering service in the electronic marketplace", Decis Support Syst, vol.

39, no. 3, pp. 371–383, 2005.

[10] R. L. Braun and H. E. Davis, "Computer-assisted audit tools and techniques: analysis and perspectives", Managerial Auditing Journal, vol. 18, no. 9, pp. 725–731, 2003.

[11] J. R. Rajalakshmi, M. Rathinraj, and M. Braveen, "Anonymizing log management process for secure logging in the cloud", in Proc. ICCPCT, India, 2014, pp. 1559–1564.

[12] W. D. Doyle, "Magnetization reversal in films with biaxial anisotropy," in 1987 Proc. INTERMAG Conf., pp. 2.2-1–2.2-6.

[13] A survey of cloud computing taxonomies: Rationale and overview, Fahad polash, Abdullah Abuhussein, sajjan shiva, University of mephis.

[14] Towards Continuous cloud service assurance for critical infrastructure, Aleksandar hudic, Thomas Hecht, Markus Tauber, Austrian institute of technology.

[15] An autonomous agent based incident detection system for cloud environments, Frank Doelitzscher, Christoph reich, Martin Knahl and Nathan Clarke, Furtwangen University- Cloud research lab,IEEE trans. on cloud computing,2011.

[16] Monitoring personal data transfers in the cloud, Anderson sasntana de oliverira,Jakub sendor,Alexander garage and Kateiline Jenatton, SAP labs, France.

[17] Way in hacking the cloud using simple techniques, https://spinbackup.com/blog/a-new-easy-way-to-hack-your-google-drive/

[18] A study on cloud computing security challenges, Santosh Bulusu and kalyan sudia, Blekinge Institute of technology, Sweden.

[19] Imperva's Hacker Intelligence Summary Report.

[20] Cloud Computing Security, wikipedia.

[21] Secuity attacks in Stand-alone computer and cloud computing: An analysis https://www.slideshare.net/mobile/dadkhah077/security-attacks-in-standalone-computer-and-cloud-computing-an-analysis.